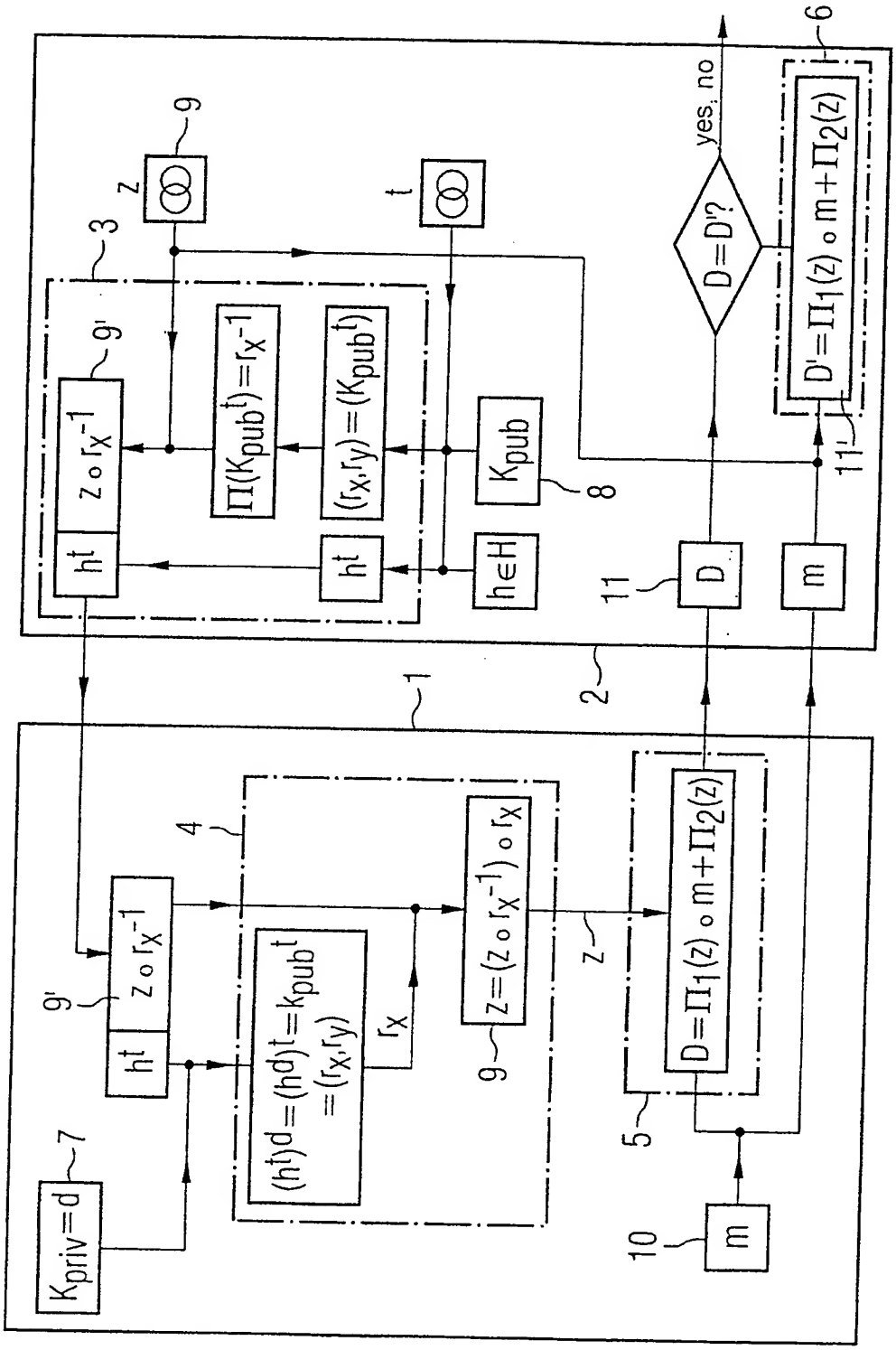
1
2
3
4
5
6
7
8
9
10
11
11'
9'
$K_{priv}=d$
h^t
$z \circ r_X^{-1}$
$(h^t)^d=(h^d)^t=k_{pub}{}^t$
$=(r_X,r_y)$
r_X
$z=(z \circ r_X^{-1}) \circ r_X$
$D=\Pi_1(z) \circ m+\Pi_2(z)$
$\Pi(K_{pub}{}^t)=r_X^{-1}$
$(r_X,r_y)=(K_{pub}{}^t)$
K_{pub}
$h \in H$
D
m
$D=D'?$
yes, no
$D'=\Pi_1(z) \circ m+\Pi_2(z)$
z
t